**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF TEXAS**
**AUSTIN DIVISION**

| | |
|---|---|
| **SOFTEX LLC**<br><br>**Plaintiff,**<br><br>**vs.**<br><br>**ABSOLUTE SOFTWARE CORP. AND ABSOLUTE SOFTWARE, INC.**<br><br>**Defendants.** | **Civil Action No. 1:22-cv-01308**<br><br>**JURY TRIAL DEMANDED** |

# COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Softex LLC ("Plaintiff") files this Complaint against Absolute Software Corp. and Absolute Software, Inc. (collectively "Absolute" or "Defendants") and alleges as follows:

## PARTIES

1. Plaintiff Softex LLC is a Delaware limited liability company having its principal place of business at 9300 Jollyville Road, Suite 201, Austin, Texas 78759.

2. Softex LLC is the owner by assignment of U.S. Patent Nos. 7,590,837 ("the '837 Patent"), 8,516,235 ("the '235 Patent"), 8,145,892 ("the '892 Patent"), 8,287,603 ("the '603 Patent"), 8,506,649 ("the '649 Patent"), 8,137,410 ("the '410 Patent"), and 8,128,710 ("the '710 Patent") (collectively "the Asserted Patents").

3. Softex, Inc. is the original named assignee to the Asserted Patents. Softex, Inc. was founded in 1992 by Mahendra Bhansali and current CEO Apurva Bhansali with a mission to provide innovative security-focused software products and solutions for computing devices. Softex, Inc. has established itself as one of the top security solution providers with innovative products focused on persistent theft detection security, enterprise single sign on, identity and

access management, and data protection of self-encrypting drives. Softex, Inc. pioneered a class of theft prevention and recovery software that is embedded on Basic Input/Output System (BIOS) chips and/or non-viewable portions of hard disk drives at the point of manufacture, and Softex, Inc. holds many patents directly related to this technology. Softex, Inc.'s persistent theft detection security software, including "TheftGuard," competed for some time with products sold by Absolute Software, Inc. and Absolute Software Corp.

4. Defendant Absolute Software Corp. is a corporation organized and existing under the laws of the Province of British Columbia, Canada, with its principal place of business located at 1055 Dunsmuir Street, Suite 1400, Vancouver, British Columbia, Canada. On information and belief, Absolute Software Corp. (including its subsidiaries) directly and/or indirectly develops, designs, manufactures, uses, distributes, markets, tests, offers to sell, and/or sells software that infringes the Asserted Patents in the United States, including in this district, and otherwise purposefully directs infringing activities to this district in connection with its software.

5. Defendant Absolute Software, Inc. is a wholly owned subsidiary of Absolute Software Corp. and is organized under the laws of the state of Washington with a principal place of business at 11401 Century Oaks Terrace, Suite 430, Austin, Texas 78758. Absolute Software, Inc. is being served through its registered agent C T Corporation System, which is located at 1999 Bryan St. Ste. 900 Dallas, TX 75201.

6. Absolute Software, Inc. is registered to do business in Texas.

7. Absolute has placed or contributed to placing infringing products such as its infringing software and computers with Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace software into the stream of commerce via an established distribution channel knowing or understanding that such products

would be sold and used in the United States, including in the Western District of Texas. On information and belief, Absolute also has derived substantial revenues from infringing acts in the Western District of Texas, including from the sale and use of infringing products such as its infringing software and computers and/or tablets using infringing software, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace software.

8. Absolute products have been known by a variety names, including "Absolute Home & Office," "Absolute Computrace Persistence," "Absolute LoJack," "LoJack for Laptops," and "Computrace." *See, e.g.*, https://homeoffice.absolute.com/support/faq/#toggle-id-3 ("Why has the product name changed from Absolute LoJack to Absolute Home & Office? A: By rebranding to Absolute Home & Office, we are bringing our Consumer/Small Business product into the Absolute brand family. This helps to reduce brand confusion and provides a better connection to our commercial solution. While we have changed the product name, it's still the same technology and Investigations Team protecting your data and device. – Absolute LoJack Premium is now Absolute Home & Office PREMIUM – Absolute LoJack Standard is now Absolute Home & Office STANDARD – Absolute Data Protect is now Absolute Home & Office BASIC."; *see also* https://homeoffice.absolute.com/support/faq/#toggle-id-2 ("What is the different between Absolute Home & Office and Computrace? A: Computrace (also called Absolute Persistence Technology) is one component of Absolute Home & Office and is available on compatible devices. This component is embedded in the firmware and once activated will self-heal our software onto the device if we are removed.").

9. Absolute was aware of Softex, Inc.'s provisional patent application since at least February 2004, aware of Softex, Inc.'s utility patent application since at least August 2006, aware

of Softex Inc.'s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the '837 Patent no later than September 2009. Specifically, Softex, Inc. wrote letters to Absolute's CEO, Mr. John Livingston, dated February 17, 2004 and August 15, 2006, informing Absolute of Softex, Inc.'s provisional and utility applications, respectively. Softex, Inc. also notified Absolute that Absolute's persistent security patent applications, which were filed more than a year after Softex, Inc.'s provisional patent application, did not identify Softex, Inc.'s patent application or provisional application. Softex, Inc.'s counsel reminded Absolute of its "duty to disclose all information known to be material to patentability" and enclosed copies of 37 C.F.R. § 1.56, Softex, Inc.'s patent application, and Softex, Inc.'s provisional patent application. Absolute was slow to respond, but in late 2007, the companies began discussing Absolute's acquisition of Softex, Inc. and/or its intellectual property. Upon information and belief, Absolute performed due diligence relating to this potential acquisition that was completed no later than February 2008. On September 15, 2009, Softex, Inc. renewed discussions with Absolute when it emailed Absolute a copy of the recently granted '837 Patent. Once again, Absolute led Softex, Inc. to believe that Absolute was interested in purchasing Softex, Inc. and its intellectual property, responding that it was "highly important that [the companies] collaborate." Upon information and belief, Absolute has actual knowledge of the remaining Asserted Patents due to above-mentioned events, as well as the citation of Softex, Inc.'s patent against Absolute's U.S. patent applications, such as 2008/0211670 and 2011/0115621, and Absolute and Softex, Inc.'s competitive and collaborative relationship including due diligence performed by Absolute no later than February 2008. Absolute also has actual knowledge of the Asserted Patents at least as early as the filing of this Complaint.

## JURISDICTION AND VENUE

10. This is an action for patent infringement under the Patent Laws of the United States, 35 U.S.C. §271.

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

12. In addition, or in the alternative, this Court has personal jurisdiction over Absolute Software Corp. under Federal Rule of Civil Procedure 4(k)(2).

13. This Court has specific personal jurisdiction over Defendants pursuant to due process and/or the Texas Long Arm Statute, at least in part, because (i) Defendants have conducted and continue to conduct business in this judicial district and (ii) Softex LLC's causes of action arise, at least in part, from Absolute's contacts with and activities in the state of Texas and this judicial district. Upon information and belief, each Defendant has committed acts of infringement within the state of Texas and this judicial district by, *inter alia*, directly and/or indirectly using, testing, selling, offering to sell, or importing products that infringe one or more claims of the Asserted Patents in this judicial district and/or importing accused products into this judicial district, including via the Internet, and inducing others to commit acts of patent infringement in this judicial district, and/or committing at least a portion of any other infringements alleged herein.

14. Defendants have committed acts within this district giving rise to this action, and have established sufficient minimum contacts with the state of Texas such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

15. Absolute has placed or contributed to placing infringing products, including the accused Absolute software products and computers using such software for additional infringing

acts, including, but not limited to,[1] its customer's branded devices, into the stream of commerce via an established distribution channel knowing or understanding that such products would be sold and used in the United States, including in the Western District of Texas. On information and belief, Absolute also has derived substantial revenues from these infringing acts in the Western District of Texas.

16. On information and belief, Absolute Software Corp. operates directly in the United States through its wholly-owned subsidiary Absolute Software, Inc., which it controls and which acts as its agent in the United States, including in the Western District of Texas.

17. Absolute Software, Inc. maintains a significant physical presence in this judicial district through its office in Austin, Texas. In 2009, Absolute stated Austin was the "ideal location" for its U.S. headquarters because "[t]he city is home to the University of Texas and the caliber of people coupled with the area's reputation," which make Austin "a great place to live and work." Absolute Software, Inc. holds an active lease on an 11,000 square foot office space in Austin, Texas through at least 2026. On information and belief, Absolute Software, Inc. employs approximately 80 people in its Austin office to design, test, market, and sell products that incorporate the Asserted Patents. On information and belief, employees in Absolute's Austin office induce customers with numerous physical operating locations in this judicial district, including Dell and HP, to buy, use, test, and sell products that infringe the Asserted Patents.

18. On information and belief, Absolute Software, Corp. has derived substantial revenues from its infringing acts in the state of Texas and this district, including from its sales of infringing products. In its 2022 Annual Information Form, which it submitted to the Canadian

[1] A list of branded devices can be found here: https://www.absolute.com/partners/device-manufacturers/ and here: https://www.absolute.com/partners/device-compatibility/

Securities Administrators, Absolute Software Corp. stated, "Absolute has historically derived the majority of its revenues from outside of Canada." Further, Absolute Software Corp. stated, "The United States is currently both Absolute's largest market and source of revenue by geographic area."

19. In addition, on information and belief, Absolute Software Corp. has, and continues to, knowingly induce infringement by others within the United States and this district by advertising, marketing, and directing products containing infringing functionality to consumers, customers, manufacturers, distributors, resellers, partners, and/or end users in the United States and by providing instructions, user manuals, advertising, and/or marketing materials that facilitate, direct, or encourage the use of infringing functionality with knowledge thereof. Additionally, on information and belief, Absolute's software that embodies the Asserted Patents is factory-embedded on devices manufactured by every major PC manufacturer[2] that are distributed throughout the United States. Absolute, for example, knowingly induces infringement by device manufacturers by encouraging manufacturers to install or have installed software on devices before shipment, and Absolute knowingly encourages end-users to install infringing software and/or activate pre-installed infringing software and use systems and methods of the Asserted Patents.

20. Absolute Software Corp. also has an interactive website available to residents in this forum that supplements its physical location and entices consumers to download infringing software and/or activate infringing software that is "[b]uilt into the BIOS or firmware during the manufacturing process of the leading device manufacturers."

21. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b), (c), and 1400(b). Venue for Defendant Absolute Software Corp., a foreign corporation, is proper in every

[2] https://www.absolute.com/partners/device-manufacturers/

judicial district in the United States, including this one. Venue is proper for Absolute Software, Inc. because Absolute Software, Inc. (1) has a regular and established place of business in this judicial district, and (2) has committed and continues to commit acts of patent infringement in this judicial district by, *inter alia*, directly and/or indirectly using, testing, selling, offering to sell, or importing products that infringe one or more claims of the Asserted Patents.

## BACKGROUND

22. Founded in 1992, Softex, Inc. provides innovative security-focused software solutions to businesses and individuals around the globe. Shortly after its founding, Softex, Inc. was invited to become one of the only software developers permitted to work with Phoenix Technologies ("Phoenix") to develop BIOSs for computer manufacturers as an Independent Authorized Developer. Softex, Inc.'s relationship with Phoenix was especially significant because available space for the BIOS is extremely limited and, at the time, Phoenix had a virtual monopoly on the development of BIOSs for Original Equipment Manufacturers (OEM) of laptop and desktop computers. Through its independent work with BIOSs, Softex, Inc. gained unique insight that allowed it to conceptualize the inventive concepts in the Asserted Patents and to develop a persistent theft detection security technology that dramatically improved and indeed changed the face of the computer security industry.

23. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. Because the memory storing the BIOS is ordinarily incorporated into motherboards at the factory by OEMs, embedding persistent theft detection security software in the BIOS can drastically improve the possibility of recovering stolen or lost devices and preventing data theft. Softex, Inc. pioneered the embedding of persistent theft detection security software into the BIOS and on hidden hard drive partitions, thus enabling computer security

systems to do things that could not be accomplished prior to Softex, Inc.'s innovative solutions. Softex, Inc. filed patent applications concerning these solutions and obtained some of the earliest patents in this field, including the Asserted Patents.

24. In the early 2000s, Softex, Inc. began promoting and marketing its proprietary persistent theft detection security technology to other software companies and OEMs. Phoenix was especially interested and asked for Softex, Inc.'s permission to demonstrate TheftGuard to OEM partners, including Dell. In May 2003, Phoenix and Absolute issued a joint press release announcing Phoenix's intent to install TheftGuard on OEM BIOSs. The press release stated, "TheftGuard is a new Core Managed Environment (cME) application that will run independent of the operating system, in the highly secure host protect area (HPA) of the hard drive" and that "TheftGuard is the first theft deterrent application that cannot be removed or replaced merely by installing another hard drive." More than a dozen news outlets covered the press release, including CNET and Business Week, calling TheftGuard a "great piece of software." Journalists also recognized the innovative nature of TheftGuard, reporting that "[s]ince TheftGuard [is] also in the BIOS, even if you remove the hard drive," Softex, Inc. would still be able to "track or disable the machine, or wipe the drive." News outlets also discussed TheftGuard's software component stored on non-visible portions of hard drives, reporting that even thieves who format hard drives are "foiled by TheftGuard's place in the [host protected] section of the hard drive, which is immune to simple reformatting tools."

25. In June 2003, a representative for Softex, Inc. contacted Absolute to discuss whether it might be interested in licensing Softex, Inc.'s proprietary, theft prevention and recovery technology. Absolute expressed interest in licensing Softex, Inc.'s intellectual property, acquiring Softex, Inc.'s intellectual property, and/or forming a strategic alliance. Discussions progressed

slowly, but in January 2004, Absolute's Vice President of Marketing and Business Development emailed Softex, Inc.'s CEO that he was "getting a lot of heat to move one way or the other" with Softex, Inc. and that he believed "the best situation for both companies would be to combine efforts." Absolute's Vice President also attached a January 12, 2004 press release from Absolute announcing that Phoenix Technologies would begin installing Absolute's "Computrace" theft prevention and recovery software in the BIOS in conjunction with device manufacturers.

26. Shortly after the January 2004 press release, Phoenix disregarded its longstanding relationship with Softex, Inc. and incorporated Absolute's infringing Computrace software into OEM BIOSs. Because of the consolidation of the OEM BIOS market and the limited space available for the BIOS, Softex, Inc. was virtually shut out of the BIOS-based, persistent theft detection security software market that it created and protected via its pioneering patents.

27. On February 17, 2004, counsel for Softex, Inc. sent Absolute a letter, notifying Absolute of Softex, Inc.'s provisional patent application, requesting that Absolute review its security software products for infringement, and requesting a meeting to discuss Absolute's licensing of Softex, Inc.'s intellectual property. Absolute did not obtain a license to Softex, Inc.'s intellectual property.

28. In the years that followed the 2004 press release, Absolute's business flourished through the marketing of infringing persistent theft detection security products to OEMs and consumers. Adding insult to injury, Absolute's customers touted the benefits of Absolute's infringing software, calling Softex, Inc.'s patented technology used by Computrace "absolutely priceless." Throughout this period, Absolute initiated meetings and took overt steps that led Softex, Inc. to believe that Absolute was interested in purchasing Softex, Inc. Absolute requested, and Softex, Inc. provided, years of financial data, information about all of Softex, Inc.'s product

offerings, and details regarding Softex, Inc.'s relationships with software companies and OEMs. Absolute told Softex, Inc. it was particularly interested in Softex, Inc.'s "best of breed, excellence in engineering" and its relationships with OEMs.

29. On August 15, 2006, counsel for Softex, Inc. sent another letter to Absolute, this time notifying Absolute that Softex, Inc. had converted the provisional patent application, about which Absolute was informed in 2004, into a conventional utility application. Softex, Inc. notified Absolute that Absolute's persistent security patent applications, which were filed more than a year after Softex, Inc.'s provisional patent application, did not identify Softex, Inc.'s patent application or provisional application. Softex, Inc.'s counsel reminded Absolute of its "duty to disclose all information known to be material to patentability" and enclosed copies of 37 C.F.R. § 1.56, Softex, Inc.'s patent application, and Softex, Inc.'s provisional patent application. Absolute was slow to respond, but in late 2007, the companies began discussing Absolute's acquisition of Softex, Inc. and/or its intellectual property.

30. In early 2008, Absolute and Softex, Inc. exchanged multiple drafts of a Letter of Intent, wherein Absolute expressed its intent to purchase Softex, Inc., including all of its intellectual property rights, for $20 million Canadian dollars, pending the parties' agreement on other terms. On information and belief, during the negotiations, Absolute performed due diligence by researching Softex, Inc.'s intellectual property rights, including the Asserted Patents and/or related applications. Absolute was, therefore, on notice of Softex, Inc.'s patent applications that published before February 2008, including the applications that resulted in the '837 Patent and the '649 Patent.

31. The parties did not reach an agreement on Absolute's acquisition of Softex, Inc.

32. On September 15, 2009, Softex, Inc. rekindled discussions with Absolute when it emailed Absolute a copy of the recently granted '837 Patent. Once again, Absolute led Softex, Inc. to believe that Absolute was interested in purchasing Softex, Inc. and its intellectual property, responding that it was "highly important that [the companies] collaborate."

33. In late 2009, Absolute proposed that it proceed toward acquiring Softex, Inc. through a two-step process. First, Absolute would enter a licensing agreement whereby Absolute would market Softex, Inc.'s "OmniPass" and "SecureDrive" software. Second, after the parties had established a working relationship, Absolute would purchase Softex, Inc. and its intellectual property.

34. In July 2010, Absolute and Softex, Inc. entered a white labeling agreement that provided Absolute with the opportunity to market Softex, Inc.'s OmniPass and SecureDrive products. After signing the licensing agreement, it became apparent that Absolute never intended to truly partner with Softex, Inc. or acquire its patents, and, on information and belief, that its purported negotiations were a pretense to permit Absolute to continue to use Softex, Inc.'s proprietary technology in its own persistent theft detection security software products while at the same time staving off the threat of litigation. Absolute sold a small number of OmniPass licenses and never sold any SecureDrive licenses. Absolute never licensed any other technology from Softex, Inc., including any technology related to the Asserted Patents, and never purchased any of Softex, Inc.'s intellectual property rights.

35. Absolute has incorporated Softex, Inc.'s technology into its products and offerings without authorization.

36. Softex, Inc. transferred all rights, title, and interest in and to the Asserted Patents to Softex LLC on August 5, 2022. The assignment was recorded on August 9, 2022 at reel/frame: 060760/0082.

## THE ASSERTED PATENTS

### U.S. PATENT NO. 7,590,837

37. On September 15, 2009, United States Patent No. 7,590,837 (the "'837 Patent") entitled "Electronic Device Security and Tracking System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '837 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '837 Patent is attached hereto as Exhibit A.

38. The '837 Patent pertains to systems for securing and tracking an electronic device. *See* Ex. A, 1:34-38. The '837 Patent discloses an electronic device security and tracking system and method (ESTSM). Such a system and method may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id.*, 1:34-42. The systems and methods of the '837 Patent are designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. *Id.*, 1:12-30. In the absence of an ESTSM, like that disclosed in the '837 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:22-28. However these means of preventing device or data theft "do not always prevent theft, are costly and once

the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:28-30. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 18:34-37. Among other things, the systems of the '837 Patent dramatically increase the effectiveness of theft prevention by using a combination of a basic input/output system (BIOS) security component, a non-viewable security component, and an application component, working in conjunction with one another to provide a persistent theft detection security solution.

39. The '837 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to a system that uses an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost device. "The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component, and a Basic Input/Output System (BIOS) component. *Id*., 2:12-17. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 17:62-64. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 17:64-18:8. The BIOS component ensures that the application component has "run properly on the previous device boot and will take

action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:8-12. Thus, by utilizing the ESTSM disclosed in the '837 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '837 Patent. Further, the systems claimed in the '837 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

40. The language of each of the claims, including Claim 1, is consistent with the inventive concepts described above, as found in the specification. For example, the electronic device security and tracking system of Claim 1 requires, among other things, "an application component to execute within an OS environment wherein said application component is configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device, and wherein said application component is configured to determine whether the electronic device has been reported stolen, based on information received from the server system," "a non-viewable security component in the electronic device … compris[ing] a validator module capable of determining whether the application component is present and … has been tampered with," "a non-volatile storage device comprising a secure area" and "a basic input/output security (BIOS) component stored in the secure area, the BIOS security component configured to check the integrity of the application component during a boot process for the electronic device." *Id*., Claim 1. In addition, Claim 1 specifies further configurations for the BIOS component—namely that the BIOS component is configured to, e.g., determine whether the non-viewable security component has been tampered

with, automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check for the application component, and prevent the electronic device from booting the OS in response to receiving a notification that the electronic device has been reported stolen. *Id.* In addition, Claim 1 specifies further configurations for the application component: "the application component is configured to notify the BIOS security component that the electronic device has been reported stolen" and that the "application component is substantially distinct from the BIOS security component and the validator component." *Id.*

41. Claim 1 is directed to a specific technical solution to the prior art problems addressed above. Claim 1 as a whole is inventive and novel, as are at least each of the identified claim limitations that require an electronic device and security tracking system capable of providing a *persistent* theft detection security solution. *Id.*, 18:13-19:7. As of the priority date of the '837 Patent, the identified claim limitations that require a specific implementation for a *persistent* theft detection security solution (such as, e.g., the claimed application component, BIOS component and/or security component configurations) were not well-understood, routine or conventional. As of the priority date of the '837 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:13-27. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:27-30. The persistent theft detection security solution of Claim 1 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the BIOS security component is configured to determine whether the non-viewable security component has been tampered with, causes the electronic device to restore the integrity of the application component in response to a negative integrity check, and

prevents the electronic device from booting the OS in response to receiving a notification that the electronic device has been stolen.

42. As evidenced by the preceding paragraphs, the ’837 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’837 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,506,649**

43. On August 13, 2013, United States Patent No. 8,506,649 (the “’649 Patent”) entitled “Electronic Device Security and Tracking System and Method,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the ’649 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’649 Patent is attached hereto as Exhibit B.

44. The’649 Patent pertains to devices, articles of manufacture, and methods for securing and tracking an electronic device, and discloses an electronic device security system and tracking system and method (“ESTSM”). *See* Ex. B, 1:34-40. Such systems and methods may comprise “a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device.” *Id.*, 1:38-40. The devices, articles of manufacture, and methods claimed in the ’649 Patent are designed, *inter alia*, to solve certain technical problems affecting users of mobile electronic devices who wish to deter

device and/or data theft. In the absence of an ESTSM like that disclosed in the '649 Patent, users of mobile electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:24-29. However, these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 18:34-37. Among other things, the devices, articles of manufacture, and methods of the '649 Patent dramatically increase the effectiveness of stolen device data recovery by using a combination of a security application that utilizes code residing within a memory area that cannot be modified by the user.

45. The '649 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to a mobile electronic device, an article of manufacture, and a method for providing security for a mobile electronic device. *Id*., 1:57-62, 2:1-8. The mobile electronic device, article of manufacture, and method include/use an electronic device security and tracking system and method (ESTSM) application stored on a memory having a changeable area and a system area that is not changeable by a user. The ESTSM may reside, at least partially, on the system area of the memory. *Id.*, 3:44-60. For example, non-viewable components of the ESTSM may reside on a protected area of the memory and periodically communicate with security service. *Id.*, 19:8-44, 26:13-16. In response to the ESTSM receiving a device-loss notification, the ESTSM disables at least one user function of the mobile electronic device while still allowing the mobile electronic

device to communicate with a security service and causes some data to be copied to a server. *Id.*, 2:16-37, 34:15-37. Thus, by utilizing the ESTSM disclosed in the '649 Patent, users can recover data from stolen devices. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '649 Patent. Further, the device, methods and article of manufacture implementations claimed in the '649 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

46. The language of each of the claims, including Claim 1, is consistent with the inventive concepts described above and found in the specification. For example, the mobile electronic device of Claim 1 requires, among other things, a security application operable to perform operations "causing the mobile electronic device to periodically communicate with the security service," "accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device," and "in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service," and "automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers" where "the security application utilizes code residing at least partially in the system area" that "cannot be modified by the user" and where "the security application receives the notification from at least one of the servers via the system area." *Id*., Claim 1.

47. Claim 1 is directed to a specific technical solution to the prior art problems addressed above. Claim 1 as a whole is inventive and novel, as are at least each of the identified claim limitations that require that the mobile electronic device be capable of providing a *persistent* theft detection security solution. As of the priority date of the '649 Patent, the identified claim limitations that require a specific implementation for a *persistent* theft detection security solution (such as, e.g., the claimed security application having code housed at least partially in the system area, which cannot be modified by a user and where the security application receives the notification from at least one of the servers via the system area that cannot be modified by a user) were not well-understood, routine or conventional. As of the priority date of the '649 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id*., 1:15-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 1 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the code for the security application is housed at least partially in the system area (which cannot be modified by a user) and, when the device is reported stolen or a request to disable is received (e.g., the device cannot be located), the security application receives the notification from at least one of the servers via the system area that cannot be modified by a user. Claim 1 additionally further improves traditional prior art security solutions because the claimed invention is operable to disable at least one user function while still communicating with the security service and automatically copy some user data from the mobile electronic device to at least one of the servers.

48. As evidenced by the preceding paragraphs, the ’649 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’649 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,516,235**

49. On August 20, 2013, United States Patent No. 8,516,235 (the “’235 Patent”) entitled “Basic Input/Output System Read Only Memory Image Integration System and Method,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the ’235 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’235 Patent is attached hereto as Exhibit C.

50. The’235 Patent pertains to systems, methods, and computer readable mediums for securing and tracking an electronic device. *See* Ex. C, 1:1-3. The ’235 Patent discloses an ESTSM. The ’235 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the systems, methods, and computer readable mediums disclosed in the ’235 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:25-31. However, these means of preventing

device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:31-33. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 16:36-38. Among other things, the systems and methods of the '235 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's memory and BIOS.

51. The '235 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the systems, methods, and computer readable mediums that include/use an ESTSM to deter electronic device theft and, if stolen or lost, empower users to disable or take other administrative actions in relation to the stolen/lost device. The ESTSM system may include an electronic device with three components. The three components may be an application component, a non-viewable component, and a BIOS component. *Id*., Fig. 47. The non-viewable component determines whether the application component is present and whether it has been tampered with. The BIOS component determines whether the non-viewable component is present and whether it has been tampered with, checks the integrity of the application component, and restores the application component's integrity if it has been compromised. This arrangement allows for a persistent application component. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 16:62-66. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application

component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 15:64-16:8. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 16:8-12. Thus, by utilizing the ESTSM disclosed in the '235 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '235 Patent. Further, the systems, methods and computer readable mediums implementations claimed in the '235 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

52. The language of each of the claims, including Claim 8, is consistent with the inventive concepts described above, as found in the specification. For example, the system of Claim 8 includes, among other things, limitations requiring "a non-viewable component," "an application component connected to the non-viewable component" that is configured a particular way and "a Basic Input/Output System (BIOS) component connected to the non-viewable component" where the BIOS component is configured a specific way and where the "application component is substantially distinct from the BIOS component and the non-viewable component." *Id*., Claim 8. In addition, "the BIOS component is configured to determine whether the non-viewable component is present," "determine whether the non-viewable component has been tampered with," "check integrity of the application component during a boot process for an electronic device," and "automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component."

*Id*., Claim 8. In addition, the "non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with." *Id*., Claim 8.

53. Claim 8 is directed to a specific technical solution to the prior art problems addressed above. Claim 8 as whole is inventive and novel, as are at least each of the identified claim limitations that require a system capable of providing a *persistent* theft detection security solution. As of the priority date of the '235 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed BIOS component and non-viewable component configurations) were not well-understood, routine or conventional. As of the priority date of the '235 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id*., 1:16-33. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:31-33. The persistent theft detection security solution of Claim 8 provides a vast improvement over traditional prior art solutions because the security features remain in an area in accessible to the user in the claimed invention at least because, e.g., the application component is substantially distinct from the BIOS component and the non-viewable component and, the BIOS security component is configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for an electronic device, and cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check.

54. As evidenced by the preceding paragraph, the '235 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer

security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '235 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,145,892**

55. On March, 27, 2012, United States Patent No. 8,145,892 (the "'892 Patent") entitled "Providing an Electronic Device Security and Tracking System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '892 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '892 Patent is attached hereto as Exhibit D.

56. The '892 Patent pertains to systems, methods, devices and apparatuses for securing and tracking an electronic device. *See* Ex. D, 1:37-41. Such systems, methods, devices and apparatuses may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id.*, 1:39-41. The '892 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the method disclosed in the '892 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:25-30. However, these means of preventing device or data theft "do not always prevent

theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:31-33. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 18:60-63. Among other things, systems and methods of the '892 Patent dramatically increases the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's memory and/or the BIOS.

57. The '892 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the use of an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost device. "The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component, and a Basic Input/Output System (BIOS) component." *Id*., 2:17-21. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 18:21-23. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:23-34. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:34-

38. Thus, by utilizing the ESTSM disclosed in the '892 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ systems and methods disclosed in the '892 Patent. Further, the systems, methods, devices and apparatuses claimed in the '892 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior. The language of each of the claims, including Claim 12, is consistent with the inventive concepts described above, as found in the specification. For example, the electronic device of Claim 12 requires, among other things, "a non-viewable component," an application component connected to the non-viewable component capable of communicating with the non-viewable component and operable to execute within the operating system environment, and "a Basic Input/Output System (BIOS) security component connected to the non-viewable component" where "the application component is substantially distinct from the BIOS component and the non-viewable component." *Id*., Claim 12. In addition, Claim 12 requires that, "after the security service has been activated," the "non-viewable component is operable to determine whether the application component is present and whether the application component has been tampered with" and the BIOS security component is operable to "determine whether the non-viewable component is present and whether the non-viewable component has been tampered with," "check integrity of the application component during a boot process for an electronic device," and "automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component." *Id*., Claim 12. In addition, Claim 12 requires that "the application component is substantially distinct from the BIOS component and the non-viewable component."

58. Claim 12 is directed to a specific technical solution to the prior art problems addressed above. Claim 12 as whole is inventive and novel, as are the identified claim limitations that require an electronic device capable of providing a *persistent* theft detection security solution. *Id.*, 18:21-19:33. As of the priority date of the '892 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, the claimed BIOS security component and non-viewable component configurations) were not well-understood, routine or conventional. As of the priority date of the '892 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:16-33. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:31-33. The persistent theft detection security solution of Claim 12 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the claimed configuration provides security and tracking for an electronic device with a non-viewable component configured to determine whether the application component is present and has been tampered with, and a BIOS security component configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for the electronic device, and cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check all whether the application component is substantially distinct from the BIOS component and non-viewable component.

59. As evidenced by the preceding paragraph, the '892 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do

things it could not do before, the '892 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,137,410**

60. On March 20, 2012, United States Patent No. 8,137,410 (the "'410 Patent") entitled "Electronic Device Disabling System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '410 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '410 Patent is attached hereto as Exhibit E.

61. The '410 Patent pertains to apparatuses and methods for securing and tracking an electronic device. *See* Ex. E, 1:36-40. Such systems and methods may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id*., 1:38-40. The'410 Patent is designed, inter alia, to solve certain technical problems affecting users of electronic devices who wish to prevent device and/or data theft. In the absence of an ESTSM like the method disclosed in the '410 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:24-30. However, these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on

viewable components of hard drives, were easily tampered with by thieves. *Id*., 2:66-3:1. Among other things, apparatuses and methods of the '410 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components associated with an application for tracking and locating the electronic device on hidden partitions of the electronic device's memory.

62. The '410 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to apparatuses and methods for providing device security. *Id*., 1:57-62, 2:1-8. The apparatuses and methods include/use memory with a hidden partition and an application component associated with tracking and locating the electronic device/apparatus. *Id.*, 2:48-3:12, 18:29-19:44. In response to determining that the application component did not operate correctly in a power-up, restoring the application component from a backup fileset. *Id*. Thus, by utilizing the ESTSM disclosed in the '410 Patent, users track and locate lost or stolen devices and thieves cannot remove the persistent tracking and locating software. *Id.* The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '410 Patent. Further, the device, methods and article of manufacture implementations claimed in the '410 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

63. The language of each of the claims, including Claim 8, is consistent with the inventive concepts described above, as found in the specification. For example, the apparatus of Claim 8 requires, among other things, a device capable of "automatically determining whether a hidden partition in the electronic device is valid," whether the "hidden partition and an application component [are] associated with tracking and locating the electronic device," and "wherein the

hidden partition comprises a non-viewable component associated with tracking and locating the electronic device." *Id*., Claim 8. In addition, Claim 8 further specifies that, in response to a determination that hidden partition is valid, the apparatus is capable of "automatically loading the non-viewable component and transferring control to the non-viewable component." *Id*., Claim 8. In addition, Claim 8 further specifies that non-viewable component is operable to "automatically determin[e] whether the application component correctly loaded during the last power-up of the electronic device" and "automatically restor[e] the application component from a backup fileset" in response to a negative determination. *Id*., Claim 8.

64. Claim 8 is directed to a specific technical solution to the prior art problems addressed above. Claim 8 as whole is inventive and novel, as are at least the identified claim limitations that require an apparatus capable of providing a *persistent* theft detection security solution. *Id.*, 2:48-3:12, 18:29-19:44. As of the priority date of the '410 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed configuration and capabilities of the hidden partition and non-viewable component) were not well-understood, routine or conventional. As of the priority date of the '410 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id*., 1:15-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 8 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the apparatus is having a hidden partition with a non-viewable component associated with tracking and locating the electronic device, where the apparatus is capable of determining whether a hidden

partition is valid in the electronic device and, if valid, loading the non-viewable component and transferring control to the non-viewable component where the non-viewable component is configured to automatically determine whether the application component operated correctly during the last power-up of the electronic device and, in response to a negative determination, automatically restoring the application component from a backup files set.

65. As evidenced by the preceding paragraph, the ’410 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’410 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,287,603**

66. On October 16, 2012, United States Patent No. 8,287,603 (the “’603 Patent”) entitled “Electronic Device With Protection From Unauthorized Utilization,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the ’603 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’603 Patent is attached hereto as Exhibit F.

67. The ’603 Patent pertains to electronic devices, articles of manufacture, and methods that prevent lost/stolen devices from booting. *See* Ex. F, 1:36-40. The electronic devices, articles of manufacture, and methods disclosed in the ’603 Patent may comprise “a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other

interaction with the stolen electronic device." *Id.*, 1:38-40. The '603 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the method disclosed in the '603 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:24-30. However, these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id.*, 2:66-3:1. Among other things, the invention disclosed in the '603 Patent dramatically increases the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's HDD and/or the BIOS.

68. The '603 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the use of an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost device. "The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component and a Basic Input/Output System (BIOS) component." *Id.*, 2:16-20. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. *Id.*, 11:4-13. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from

the electronic device. *Id*., 18:13-15. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:15-26. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:26-30. Thus, by utilizing the ESTSM disclosed in the '603 Patent, users can deter theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the systems and methods disclosed in the '603 Patent. Further, the electronic device, articles of manufacture, and methods claimed in the '603 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

69. The language of each of the claims, including Claim 18, is consistent with the inventive concepts described above, as found in the specification. For example, Claim 18 requires, among other things, an electronic device capable of "executing an application component … configured to automatically ascertained whether the electronic device has been reported stolen based on information received from a server system," "automatically determining whether the application component is operating correctly," "in response to a determination that the application component is operating correctly, automatically providing a basic input/output system (BIOS) component of the electronic device with information indicating that the application component is operating correctly" and "during a subsequent boot process for the electronic device, automatically

preventing the electronic device from completing the boot process if the BIOS component does not find the information from the application component indicating that the application component was operating correctly." *Id*., Claim 18.

70. Claim 18 is directed to a specific technical solution to the prior art problems addressed above. Claim 18 as whole is inventive and novel, as are at least the identified claim limitations that requiring that electronic device be capable of providing a persistent theft detection security solution. *Id*., 18:13-19:27. As of the priority date of the '603 Patent, the identified limitations of Claim 18 that require a specific implementation for a persistent theft detection security solution (such as, executing the application component as claimed and automatically determining whether it is operating correctly, automatically providing a BIOS component with information it is operating correctly, and, during a subsequent boot process, preventing the electronic device from completing the boot process if the BIOS component does not find the required information from the application component) were not well-understood, routine or conventional. As of the priority date of the '603 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id*., 1:15-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 18 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the electronic device is provided with software for protecting the electronic device for unauthorized utilization where, in response to a determination that the application component is operating correctly, automatically providing the BIOS component with information indicating the application component is operating correctly and, during a subsequent

boot process, preventing the electronic device from completing the boot process if the BIOS component does not find the information from the application component indicating that the application component was operating correctly.

71. As evidenced by the preceding paragraph, the ’603 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’603 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

**U.S. PATENT NO. 8,128,710**

72. On March 6, 2012, United States Patent No. 8,128,710 (the “’710 Patent”) entitled “Electronic Device Security System and Method,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the ’710 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’710 Patent is attached hereto as Exhibit G.

73. The’710 Patent pertains to systems, methods, and articles of manufacture for securing and tracking an electronic device. *See* Ex. G, 1:15-4:29. The ’710 Patent discloses an ESTSM. The ’710 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the systems, methods, and articles of manufacture disclosed in the ’710 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical

attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:24-32. However, these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 19:2-4. Among other things, the systems and methods of the '710 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's memory and BIOS.

74. The '710 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the systems, methods, and articles of manufacture that include/use an ESTSM to deter electronic device theft and, if stolen or lost, empower users to disable or take other administrative actions in relation to the stolen/lost device. The ESTSM system may include an electronic device with three components. The three components may be an application component, a non-viewable component, and a BIOS component. *Id*., Fig. 47. The non-viewable component determines whether the application component is present and whether it has been tampered with. The BIOS component determines whether the non-viewable component is present and whether it has been tampered with, checks the integrity of the application component, and restores the application component's integrity if it has been compromised. This arrangement allows for a persistent application component. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 19:28-30. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image

located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:29-46. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*. Thus, by utilizing the ESTSM disclosed in the '710 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. And, in response to a theft, the user can wipe the non-volatile storage device to secure their data. *Id.*, 16:26-41; *see also id.*, 4:61-5:24, 9:9-15, 18:22-28, 24:15-22, 27:35-41. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '710 Patent. Further, the systems, methods and articles of manufacture implementations claimed in the '710 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

75. The language of each of the claims, including Claim 2, is consistent with the inventive concepts described above, as found in the specification. For example, the system of Claim 2 includes, among other things, limitations requiring "a non-viewable component," "an application component connected to the non-viewable component" that is configured a particular way and "a Basic Input/Output System (BIOS) component connected to the non-viewable component" where the BIOS component is configured a specific way and where the "application component is substantially distinct from the BIOS component and the non-viewable component." *Id*., Claim 2. In addition, "the BIOS component is configured to determine whether the non-

viewable component is present," "determine … whether the non-viewable component has been tampered with," "check integrity of the application component during a boot process for the electronic device," and "automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component." *Id*., Claim 2. In addition, the "non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with." *Id*., Claim 2. The system is also operable to perform operations, such as "causing to be presented, by a device other than the electronic device, an option to confirm that the non-volatile storage device of the electronic device is to be erased; accepting, from the device other than the electronic device, input to confirm that the non-volatile storage device is to be erased; and after receiving the report that the electronic device has been stolen, causing the electronic device to erase the non-volatile storage device." *Id*., Claim 2.

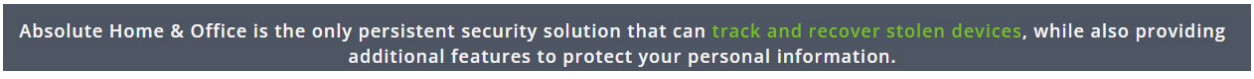
76. Claim 2 is directed to a specific technical solution to the prior art problems addressed above. Claim 2 as whole is inventive and novel, as are at least each of the identified claim limitations that require a system capable of providing a *persistent* theft detection security solution with the ability to wipe data on a compromised device. As of the priority date of the '710 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed BIOS component and non-viewable component configurations alone or together with the ability to erase data from a stolen device) were not well-understood, routine or conventional. As of the priority date of the '710 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id*., 1:16-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or

recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 2 provides a vast improvement over traditional prior art solutions because the security features remain in an area in accessible to the user in the claimed invention at least because, e.g., the application component is substantially distinct from the BIOS component and the non-viewable component and, the BIOS security component is configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for an electronic device, cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check, and cause the electronic device to erase the non-volatile storage device.

77. As evidenced by the preceding paragraph, the '710 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '710 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

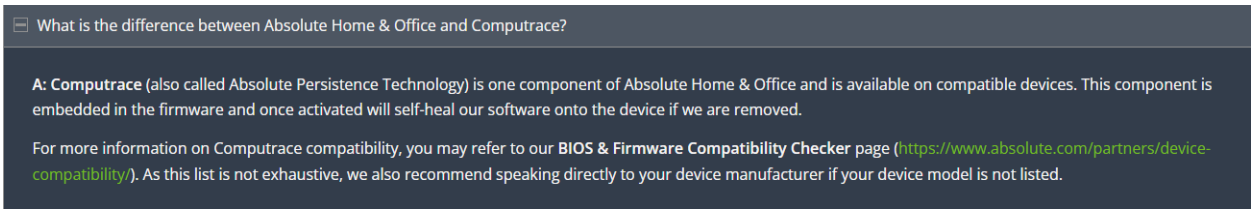
**ABSOLUTE's INFRINGING PRODUCTS AND SERVICES**

78. Upon information and belief, Absolute has infringed and continues to infringe one or more claims of the Asserted Patents, as shown below, by making, testing, using, offering to sell, and selling one or more infringing products including Absolute Home & Office. Absolute Home & Office has also been marketed as LoJack for Laptops or Absolute LoJack. https://homeoffice.absolute.com/support/faq/#toggle-id-3. Absolute markets the Absolute Home & Office as a "persistent security solution that can track and recover stolen devices."




https://homeoffice.absolute.com/.

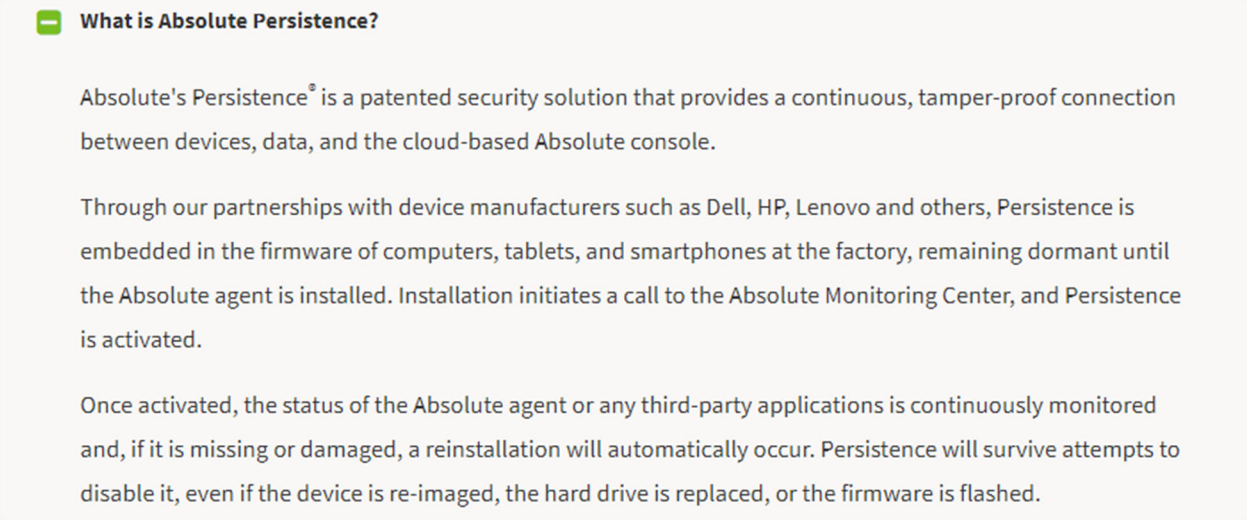
79. Absolute Home & Office includes a component called Computrace (also called Absolute Persistence Technology) that is "embedded in the firmware and once activated will self-heal our software onto the device if we are removed."




https://homeoffice.absolute.com/support/faq/#toggle-id-2.

80. Absolute Home & Office includes services residing, at least in part, on a server, allowing a user to view a device's location on a map, remotely lock a device, and remotely delete some or all files from a device.

81. The Absolute Persistence component of Absolute Home & Office (also known as Computrace) is installed on computers/tablets during the manufacturing process.



**What is Absolute Persistence?**

Absolute's Persistence® is a patented security solution that provides a continuous, tamper-proof connection between devices, data, and the cloud-based Absolute console.

Through our partnerships with device manufacturers such as Dell, HP, Lenovo and others, Persistence is embedded in the firmware of computers, tablets, and smartphones at the factory, remaining dormant until the Absolute agent is installed. Installation initiates a call to the Absolute Monitoring Center, and Persistence is activated.

Once activated, the status of the Absolute agent or any third-party applications is continuously monitored and, if it is missing or damaged, a reinstallation will automatically occur. Persistence will survive attempts to disable it, even if the device is re-imaged, the hard drive is replaced, or the firmware is flashed.

https://www.absolute.com/platform/editions/.

**COUNT 1**
**INFRINGEMENT OF U.S. PATENT NO. 7,590,837**

82. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-81 above as if fully set herein.

83. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the ’837 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.’s provisional patent application (to which the ’837 Patent claims priority) since at least February 2004, aware of Softex, Inc.’s conventional utility patent application since at least August 2006, aware of Softex, Inc.’s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the ’837 Patent since at least September 2009. Therefore, the entirety of Absolute’s infringement is knowing and willful.

84. With knowledge of the ’837 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 1 of the ’837 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home &

Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. H.

85. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 1 of the'837 Patent, either literally or equivalently.

86. With knowledge of the '837 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '837 Patent, including at least Claim 1. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 1 of the '837 Patent, as described in Ex. H. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

87. Upon information and belief, Absolute's acts of infringing the '837 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

88. As a direct and proximate consequence of Absolute's infringement of the '837 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

**COUNT 2**
**INFRINGEMENT OF U.S. PATENT NO. 8,506,649**

89. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-88 above as if fully set herein.

90. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the '649 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.'s provisional patent application (to which the '649 Patent claims priority) since at least February 2004, aware of Softex, Inc.'s conventional utility patent application since at least August 2006, aware of Softex, Inc.'s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the '837 Patent since at least September 2009. Therefore, the entirety of Absolute's infringement is knowing and willful.

91. With knowledge of the '649 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent Claim 1 of the '649 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. I.

92. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 1 of the'649 Patent, either literally or equivalently.

93. With knowledge of the '649 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or

AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '649 Patent, including at least Claim 1. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 1 of the '649 Patent, as described in Ex. I. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

94. Upon information and belief, Absolute's acts of infringing the '649 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

95. As a direct and proximate consequence of Absolute's infringement of the '649 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

**COUNT 3**
**INFRINGEMENT OF U.S. PATENT NO. 8,516,235**

96. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-95 above as if fully set herein.

97. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the '235 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.'s provisional patent application (to which the '235 Patent claims priority) since at least February 2004, aware of Softex, Inc.'s conventional utility patent application since at least August 2006, aware of Softex, Inc.'s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the

issuance of the ’837 Patent since at least September 2009. Therefore, the entirety of Absolute’s infringement is knowing and willful.

98. With knowledge of the ’235 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 8 of the ’235 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. J.

99. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 8 of the’235 Patent, either literally or equivalently.

100. With knowledge of the ’235 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’235 Patent, including at least Claim 8. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 8 of the ’235 Patent, as described in Ex. J. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

101. Upon information and belief, Absolute's acts of infringing the '235 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

102. As a direct and proximate consequence of Absolute's infringement of the '235 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

**COUNT 4**
**INFRINGEMENT OF U.S. PATENT NO. 8,145,892**

103. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-102 above as if fully set herein.

104. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the '892 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.'s provisional patent application (to which the '892 Patent claims priority) since at least February 2004, aware of Softex, Inc.'s conventional utility patent application since at least August 2006, aware of Softex, Inc.'s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the '837 Patent since at least September 2009. Therefore, the entirety of Absolute's infringement is knowing and willful.

105. With knowledge of the '892 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent Claim 12 of the '892 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. K.

106. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 12 of the'892 Patent, either literally or equivalently.

107. With knowledge of the '892 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '892 Patent, including at least Claim 12. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 12 of the '892 Patent, as described in Ex. K. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

108. Upon information and belief, Absolute's acts of infringing the '892 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

109. As a direct and proximate consequence of Absolute's infringement of the '892 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

## COUNT 5
## INFRINGEMENT OF U.S. PATENT NO. 8,137,410

110. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-109 above as if fully set herein.

111. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the ’410 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.’s provisional patent application (to which the ’410 Patent claims priority) since at least February 2004, aware of Softex, Inc.’s conventional utility patent application since at least August 2006, aware of Softex, Inc.’s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the ’837 Patent since at least September 2009. Therefore, the entirety of Absolute’s infringement is knowing and willful.

112. With knowledge of the ’410 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent Claim 8 of the ’410 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. L.

113. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 8 of the’410 Patent, either literally or equivalently.

114. With knowledge of the ’410 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’410 Patent, including at least Claim 8. Absolute has actively induced direct infringement by providing, *inter alia*, functionality,

instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 8 of the '410 Patent, as described in Ex. L. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

115. Upon information and belief, Absolute's acts of infringing the '410 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

116. As a direct and proximate consequence of Absolute's infringement of the '410 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

**COUNT 6**
**INFRINGEMENT OF U.S. PATENT NO. 8,287,603**

117. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-116 above as if fully set herein.

118. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the '603 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.'s provisional patent application (to which the '603 Patent claims priority) since at least February 2004, aware of Softex, Inc.'s conventional utility patent application since at least August 2006, aware of Softex, Inc.'s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the '837 Patent since at least September 2009. Therefore, the entirety of Absolute's infringement is knowing and willful.

119. With knowledge of the '603 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent Claim 18 of

the ’603 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. M.

120. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 18 of the’603 Patent, either literally or equivalently.

121. With knowledge of the ’603 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’603 Patent, including at least Claim 18. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 18 of the ’603 Patent, as described in Ex. M. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

122. Upon information and belief, Absolute’s acts of infringing the ’603 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC’s patent rights.

123. As a direct and proximate consequence of Absolute’s infringement of the ’603 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

**COUNT 7**
**INFRINGEMENT OF U.S. PATENT NO. 8,128,710**

124. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-123 above as if fully set herein.

125. Upon information and belief, Absolute has had actual and/or constructive notice of its infringement of the ’710 Patent since Absolute began marketing infringing persistent security software, having been aware of Softex, Inc.’s provisional patent application (to which the ’710 Patent claims priority) since at least February 2004, aware of Softex, Inc.’s conventional utility patent application since at least August 2006, aware of Softex, Inc.’s entire intellectual property portfolio through due diligence Absolute performed no later than February 2008, and aware of the issuance of the ’837 Patent since at least September 2009. Therefore, the entirety of Absolute’s infringement is knowing and willful.

126. With knowledge of the ’710 Patent, Absolute has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent Claim 2 of the ’710 Patent by making, testing, using, selling, and/or offering for sale its Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, AKA Computrace in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. N.

127. Absolute products, including Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace, meet each and every element of at least Claim 2 of the’710 Patent, either literally or equivalently.

128. With knowledge of the ’710 Patent, Absolute has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging its customers to activate Absolute Home & Office, AKA Absolute Computrace Persistence, AKA Absolute LoJack, AKA LoJack for Laptops, and/or

AKA Computrace onto computers sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '710 Patent, including at least Claim 2. Absolute has actively induced direct infringement by providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause its customers to directly infringe at least Claim 2 of the '710 Patent, as described in Ex. N. Upon information and belief, Absolute has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by its customers.

129. Upon information and belief, Absolute's acts of infringing the '710 Patent have been willful and undertaken in knowing and deliberate disregard of Softex LLC's patent rights.

130. As a direct and proximate consequence of Absolute's infringement of the '710 Patent, Softex LLC has suffered damages in an amount not yet determined for which Absolute is entitled to relief.

## DEMAND FOR JURY TRIAL

131. Plaintiff hereby demands a jury trial for all issues so triable.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. Declare that Defendants have infringed, and continue to infringe, one or more claims of the Asserted Patents, contributed to the infringement of the Asserted Patents, and/or induced the infringement of the Asserted Patents;

B. Enter judgment that Defendants' acts of patent infringement are willful;

C. Award damages no less than a reasonable royalty to Plaintiff arising out of this infringement of the Asserted Patents, including enhanced damages for willful infringement

pursuant to 35 U.S.C. § 284 and prejudgment and post-judgment interest, in an amount according to proof;

D. Award attorneys' fees to Plaintiffs pursuant to 35 U.S.C. §§ 284 and 285 or as otherwise permitted by law;

E. Award Plaintiff the interest and costs incurred in this action; and

F. Grant Plaintiff such other and further relief, including equitable relief, as the Court deems just and proper.

Dated: December 14, 2022

Respectfully submitted,

**MCKOOL SMITH, P.C.**

*/s/ Blair M. Jacobs*

Blair M. Jacobs (WDTX. Bar No. 32010)
bjacobs@McKoolSmith.com
Christina A. Ondrick (WDTX. Bar No. 494625)
condrick@McKoolSmith.com
John S. Holley (SBN 24078678)
jholley@McKoolSmith.com
Steven W. Peters (DC Bar No. 176041
*pro hac vice to be submitted*)
speters@McKoolSmith.com
1999 K Street, NW Suite 600
Washington, D.C. 20006
Telephone: (202) 370-8300
Facsimile: (202) 370-8344

John B. Campbell (SBN 24036314)
jcampbell@McKoolSmith.com
**MCKOOL SMITH, P.C.**
303 Colorado Street, Suite 2100
Austin, TX 78701
Telephone: (512) 692-8700
Facsimile: (512) 692-8744

Casey L. Shomaker (SBN 24110359)
cshomaker@McKoolSmith.com
Matthew Folks (SBN 24116368)
mfolks@McKoolSmith.com
**MCKOOL SMITH, P.C.**
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: (214) 978-4218
Facsimile: (214) 978-4044

***ATTORNEYS FOR PLAINTIFF SOFTEX LLC***